Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP2005/017305

International filing date: 20 September 2005 (20.09.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-298247
Filing date: 12 October 2004 (12.10.2004)

Date of receipt at the International Bureau: 28 October 2005 (28.10.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 Date of Application:	２００４年１０月１２日
出願番号 Application Number:	特願２００４－２９８２４７
パリ条約による外国への出願に用いる優先権の主張の基礎となる出願の国コードと出願番号 The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is	ＪＰ２００４－２９８２４７
出願人 Applicant(s):	日本電信電話株式会社

２００５年１０月１２日

特許庁長官
Commissioner,
Japan Patent Office

中嶋　誠

【書類名】　特許願
【整理番号】　NTTH166077
【提出日】　平成16年10月12日
【あて先】　特許庁長官殿
【国際特許分類】　H04L 12/46
【発明者】
　【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
　【氏名】　瀬林　克啓
【発明者】
　【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
　【氏名】　倉上　弘
【発明者】
　【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
　【氏名】　副島　裕司
【発明者】
　【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
　【氏名】　エリック　チェン
【発明者】
　【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
　【氏名】　冨士　仁
【特許出願人】
　【識別番号】　000004226
　【氏名又は名称】　日本電信電話株式会社
【代理人】
　【識別番号】　100089118
　【弁理士】
　【氏名又は名称】　酒井　宏明
【選任した代理人】
　【識別番号】　100114306
　【弁理士】
　【氏名又は名称】　中辻　史郎
【手数料の表示】
　【予納台帳番号】　036711
　【納付金額】　16,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　0310351

【書類名】特許請求の範囲
【請求項１】
パケットの通過を制御するためのシグネチャを隣接中継装置から受信し、当該受信したシグネチャを他の隣接中継装置に送信する中継装置であって、
前記隣接中継装置から受信したシグネチャの条件を満たすパケットを監視して、当該パケットによる攻撃の有無を判定する攻撃有無判定手段と、
前記攻撃有無判定手段によって攻撃有りと判定された場合に、前記隣接中継装置から受信したシグネチャを前記他の隣接中継装置に送信するシグネチャ送信手段と、
を備えたことを特徴とする中継装置。
【請求項２】
前記攻撃有無判定手段は、前記隣接中継装置から受信したシグネチャの条件を満たす単位時間内のパケット数が所定の閾値を超過したか否かを判定するパケット数判定手段を備え、
前記シグネチャ送信手段は、前記パケット数判定手段によって前記単位時間内のパケット数が所定の閾値を超過したと判定された場合に、前記隣接中継装置から受信したシグネチャを前記他の隣接中継装置に送信することを特徴とする請求項１に記載の中継装置。
【請求項３】
前記攻撃有無判定手段は、前記パケット数判定手段によって前記単位時間内のパケット数が所定の閾値を超過したと判定された場合に、当該所定の閾値を連続して超過した回数が所定値を超過したか否かを判定する連続超過回数判定手段をさらに備え、
前記シグネチャ送信手段は、前記連続超過回数判定手段によって所定値を超過したと判定された場合に、前記隣接中継装置から受信したシグネチャを前記他の隣接中継装置に送信することを特徴とする請求項２に記載の中継装置。
【請求項４】
前記シグネチャ送信手段は、全ての隣接中継装置のなかから前記シグネチャを送信した隣接中継装置を除いた他の隣接中継装置に対して前記シグネチャを送信することを特徴とする請求項１、２または３に記載の中継装置。
【請求項５】
パケットの通過を制御するためのシグネチャを隣接中継装置から受信し、当該受信したシグネチャを他の隣接中継装置に送信する複数の中継装置からなるネットワーク攻撃防御システムであって、
前記中継装置は、
前記隣接中継装置から受信したシグネチャの条件を満たすパケットを監視して、当該パケットによる攻撃の有無を判定する攻撃有無判定手段と、
前記攻撃有無判定手段によって攻撃有りと判定された場合に、前記隣接中継装置から受信したシグネチャを前記他の隣接中継装置に送信するシグネチャ送信手段と、
を備えたことを特徴とするネットワーク攻撃防御システム。
【請求項６】
パケットの通過を制御するためのシグネチャを隣接中継装置から受信し、当該受信したシグネチャを他の隣接中継装置に送信する中継装置における中継方法であって、
前記隣接中継装置から受信したシグネチャの条件を満たすパケットを監視して、当該パケットによる攻撃の有無を判定する攻撃有無判定工程と、
前記攻撃有無判定工程によって攻撃有りと判定された場合に、前記隣接中継装置から受信したシグネチャを前記他の隣接中継装置に送信するシグネチャ送信工程と、
を含んだことを特徴とする中継方法。
【請求項７】
前記攻撃有無判定工程は、前記隣接中継装置から受信したシグネチャの条件を満たす単位時間内のパケット数が所定の閾値を超過したか否かを判定するパケット数判定工程を含み、
前記シグネチャ送信工程は、前記パケット数判定工程によって前記単位時間内のパケッ

ト数が所定の閾値を超過したと判定された場合に、前記隣接中継装置から受信したシグネチャを前記他の隣接中継装置に送信することを特徴とする請求項６に記載の中継方法。
【請求項８】
前記攻撃有無判定工程は、前記パケット数判定工程によって前記単位時間内のパケット数が所定の閾値を超過したと判定された場合に、当該所定の閾値を連続して超過した回数が所定値を超過したか否かを判定する連続超過回数判定工程をさらに含み、
前記シグネチャ送信工程は、前記連続超過回数判定工程によって所定値を超過したと判定された場合に、前記隣接中継装置から受信したシグネチャを前記他の隣接中継装置に送信することを特徴とする請求項７に記載の中継方法。
【請求項９】
前記シグネチャ送信工程は、全ての隣接中継装置のなかから前記シグネチャを送信した隣接中継装置を除いた他の隣接中継装置に対して前記シグネチャを送信することを特徴とする請求項６、７または８に記載の中継方法。
【請求項１０】
パケットの通過を制御するためのシグネチャを隣接中継装置から受信し、当該受信したシグネチャを他の隣接中継装置に送信する中継装置としてのコンピュータに実行させる中継プログラムであって、
前記隣接中継装置から受信したシグネチャの条件を満たすパケットを監視して、当該パケットによる攻撃の有無を判定する攻撃有無判定手順と、
前記攻撃有無判定手順によって攻撃有りと判定された場合に、前記隣接中継装置から受信したシグネチャを前記他の隣接中継装置に送信するシグネチャ送信手順と、
をコンピュータに実行させることを特徴とする中継プログラム。
【請求項１１】
前記攻撃有無判定手順は、前記隣接中継装置から受信したシグネチャの条件を満たす単位時間内のパケット数が所定の閾値を超過したか否かを判定するパケット数判定手順をコンピュータに実行させ、
前記シグネチャ送信手順は、前記パケット数判定手順によって前記単位時間内のパケット数が所定の閾値を超過したと判定された場合に、前記隣接中継装置から受信したシグネチャを前記他の隣接中継装置に送信することを特徴とする請求項１０に記載の中継プログラム。
【請求項１２】
前記攻撃有無判定手順は、前記パケット数判定手順によって前記単位時間内のパケット数が所定の閾値を超過したと判定された場合に、当該所定の閾値を連続して超過した回数が所定値を超過したか否かを判定する連続超過回数判定手順をさらにコンピュータに実行させ、
前記シグネチャ送信手順は、前記連続超過回数判定手順によって所定値を超過したと判定された場合に、前記隣接中継装置から受信したシグネチャを前記他の隣接中継装置に送信することを特徴とする請求項１１に記載の中継プログラム。
【請求項１３】
前記シグネチャ送信手順は、全ての隣接中継装置のなかから前記シグネチャを送信した隣接中継装置を除いた他の隣接中継装置に対して前記シグネチャを送信することを特徴とする請求項１０、１１または１２に記載の中継プログラム。

【書類名】明細書
【発明の名称】中継装置、中継方法および中継プログラム並びにネットワーク攻撃防御システム
【技術分野】
【０００１】
この発明は、パケットの通過を制御するためのシグネチャを隣接中継装置から受信し、当該受信したシグネチャを他の隣接中継装置に送信する中継装置、中継方法および中継プログラム並びにネットワーク攻撃防御システムに関する。
【背景技術】
【０００２】
従来より、防御対象であるコンピュータが接続されたネットワーク上に複数の中継装置を有し、ＤｏＳ（Denial of Service）攻撃またはＤＤｏＳ（Distributed Denial of Service）攻撃を受けるコンピュータを防御するネットワーク攻撃防御システムが知られている。例えば、特許文献１（特開２００３－２８３５５４号公報）や特許文献２（特開２００３－２８３５７２号公報）に開示されたネットワーク攻撃防御システムでは、中継装置において、予め決められた攻撃容疑パケットの検出条件に通信トラヒックが合致するか否かをチェックする。そして、合致したトラヒックを検出した場合に、中継装置は、検出された攻撃容疑パケットの伝送帯域制限値を表すシグネチャを生成して隣接中継装置（隣接関係をもつ中継装置）へ送信するとともに、以後、シグネチャによって識別される攻撃容疑パケットの伝送帯域を制限する処理を行う。
【０００３】
一方、シグネチャを受信した中継装置（隣接中継装置）では、通過するパケットの伝送帯域をシグネチャによって表される伝送帯域制限値に制限するとともに、さらに上流の隣接中継装置に対してシグネチャを送信する。つまり、シグネチャを受信した各中継装置がシグネチャの送信を繰り返すことで、ネットワーク上の全ての中継装置が同様のシグネチャに基づいてパケットを処理し、これによって、各中継装置を通過するパケットの伝送帯域をシグネチャが示す伝送帯域制限値に制限する。なお、上流または下流の中継装置とは、隣接中継装置であり、かつ攻撃容疑パケットが流入する方向に対する中継装置である。
【０００４】
さらに、一定時間経過後、攻撃を検出した中継装置は、各隣接中継装置から攻撃容疑パケットの平均入力伝送帯域値を受信し、各隣接中継装置における平均入力伝送帯域の比率により伝送帯域制限調整値を算出し、算出した伝送帯域制限調整値を隣接中継装置に送信する。そして、かかる伝送帯域制限調整値を受信した中継装置は、受信した伝送帯域制限調整値に基づいて伝送帯域制限を調整しながら、さらに上流の隣接中継装置に伝送帯域制限調整値を送信する。つまり、伝送帯域制限調整値を受信した各中継装置が伝送帯域制限調整値の送信を繰り返すことで、ネットワーク上の全ての中継装置が同様の伝送帯域制限調整値を受信し、受信した伝送帯域制限調整値に基づいて伝送帯域制限を調整する。
【０００５】
【特許文献１】特開２００３－２８３５５４号公報
【特許文献２】特開２００３－２８３５７２号公報
【発明の開示】
【発明が解決しようとする課題】
【０００６】
しかしながら、上記した従来の技術は、ネットワーク上の特定の中継装置が容疑のかかる攻撃を検出した場合でも、ネットワーク攻撃防御システムを構成する全ての中継装置に対してシグネチャを送信するので、攻撃容疑パケットの通信経路上にない中継装置にまでもシグネチャを送信してしまう結果、容疑のかかる攻撃を検出したとき等の各中継装置にかかる処理負荷が高くなってしまうという問題があった。
【０００７】
そこで、この発明は、上述した従来技術の課題を解決するためになされたものであり、

ネットワーク上にある各中継装置の処理負荷を低減し、パケットの規制に関する処理を効率良く行うことが可能な中継装置、中継方法および中継プログラム並びにネットワーク攻撃防御システムを提供することを目的とする。

【課題を解決するための手段】

【０００８】

上述した課題を解決し、目的を達成するため、請求項１に係る発明は、パケットの通過を制御するためのシグネチャを隣接中継装置から受信し、当該受信したシグネチャを他の隣接中継装置に送信する中継装置であって、前記隣接中継装置から受信したシグネチャの条件を満たすパケットを監視して、当該パケットによる攻撃の有無を判定する攻撃有無判定手段と、前記攻撃有無判定手段によって攻撃有りと判定された場合に、前記隣接中継装置から受信したシグネチャを前記他の隣接中継装置に送信するシグネチャ送信手段と、を備えたことを特徴とする。

【０００９】

また、請求項２に係る発明は、上記の発明において、前記攻撃有無判定手段は、前記隣接中継装置から受信したシグネチャの条件を満たす単位時間内のパケット数が所定の閾値を超過したか否かを判定するパケット数判定手段を備え、前記シグネチャ送信手段は、前記パケット数判定手段によって前記単位時間内のパケット数が所定の閾値を超過したと判定された場合に、前記隣接中継装置から受信したシグネチャを前記他の隣接中継装置に送信することを特徴とする。

【００１０】

また、請求項３に係る発明は、上記の発明において、前記攻撃有無判定手段は、前記パケット数判定手段によって前記単位時間内のパケット数が所定の閾値を超過したと判定された場合に、当該所定の閾値を連続して超過した回数が所定値を超過したか否かを判定する連続超過回数判定手段をさらに備え、前記シグネチャ送信手段は、前記連続超過回数判定手段によって所定値を超過したと判定された場合に、前記隣接中継装置から受信したシグネチャを前記他の隣接中継装置に送信することを特徴とする。

【００１１】

また、請求項４に係る発明は、上記の発明において、前記シグネチャ送信手段は、全ての隣接中継装置のなかから前記シグネチャを送信した隣接中継装置を除いた他の隣接中継装置に対して前記シグネチャを送信することを特徴とする。

【００１２】

また、請求項５に係る発明は、パケットの通過を制御するためのシグネチャを隣接中継装置から受信し、当該受信したシグネチャを他の隣接中継装置に送信する複数の中継装置からなるネットワーク攻撃防御システムであって、前記中継装置は、前記隣接中継装置から受信したシグネチャの条件を満たすパケットを監視して、当該パケットによる攻撃の有無を判定する攻撃有無判定手段と、前記攻撃有無判定手段によって攻撃有りと判定された場合に、前記隣接中継装置から受信したシグネチャを前記他の隣接中継装置に送信するシグネチャ送信手段と、を備えたことを特徴とする。

【００１３】

また、請求項６に係る発明は、パケットの通過を制御するためのシグネチャを隣接中継装置から受信し、当該受信したシグネチャを他の隣接中継装置に送信する中継装置における中継方法であって、前記隣接中継装置から受信したシグネチャの条件を満たすパケットを監視して、当該パケットによる攻撃の有無を判定する攻撃有無判定工程と、前記攻撃有無判定工程によって攻撃有りと判定された場合に、前記隣接中継装置から受信したシグネチャを前記他の隣接中継装置に送信するシグネチャ送信工程と、を含んだことを特徴とする。

【００１４】

また、請求項７に係る発明は、上記の発明において、前記攻撃有無判定工程は、前記隣接中継装置から受信したシグネチャの条件を満たす単位時間内のパケット数が所定の閾値を超過したか否かを判定するパケット数判定工程を含み、前記シグネチャ送信工程は、前

記パケット数判定工程によって前記単位時間内のパケット数が所定の閾値を超過したと判定された場合に、前記隣接中継装置から受信したシグネチャを前記他の隣接中継装置に送信することを特徴とする。

【００１５】

また、請求項８に係る発明は、上記の発明において、前記攻撃有無判定工程は、前記パケット数判定工程によって前記単位時間内のパケット数が所定の閾値を超過したと判定された場合に、当該所定の閾値を連続して超過した回数が所定値を超過したか否かを判定する連続超過回数判定工程をさらに含み、前記シグネチャ送信工程は、前記連続超過回数判定工程によって所定値を超過したと判定された場合に、前記隣接中継装置から受信したシグネチャを前記他の隣接中継装置に送信することを特徴とする。

【００１６】

また、請求項９に係る発明は、上記の発明において、前記シグネチャ送信工程は、全ての隣接中継装置のなかから前記シグネチャを送信した隣接中継装置を除いた他の隣接中継装置に対して前記シグネチャを送信することを特徴とする。

【００１７】

また、請求項１０に係る発明は、パケットの通過を制御するためのシグネチャを隣接中継装置から受信し、当該受信したシグネチャを他の隣接中継装置に送信する中継装置としてのコンピュータに実行させる中継プログラムであって、前記隣接中継装置から受信したシグネチャの条件を満たすパケットを監視して、当該パケットによる攻撃の有無を判定する攻撃有無判定手順と、前記攻撃有無判定手順によって攻撃有りと判定された場合に、前記隣接中継装置から受信したシグネチャを前記他の隣接中継装置に送信するシグネチャ送信手順と、をコンピュータに実行させることを特徴とする。

【００１８】

また、請求項１１に係る発明は、上記の発明において、前記攻撃有無判定手順は、前記隣接中継装置から受信したシグネチャの条件を満たす単位時間内のパケット数が所定の閾値を超過したか否かを判定するパケット数判定手順をコンピュータに実行させ、前記シグネチャ送信手順は、前記パケット数判定手順によって前記単位時間内のパケット数が所定の閾値を超過したと判定された場合に、前記隣接中継装置から受信したシグネチャを前記他の隣接中継装置に送信することを特徴とする。

【００１９】

また、請求項１２に係る発明は、上記の発明において、前記攻撃有無判定手順は、前記パケット数判定手順によって前記単位時間内のパケット数が所定の閾値を超過したと判定された場合に、当該所定の閾値を連続して超過した回数が所定値を超過したか否かを判定する連続超過回数判定手順をさらにコンピュータに実行させ、前記シグネチャ送信手順は、前記連続超過回数判定手順によって所定値を超過したと判定された場合に、前記隣接中継装置から受信したシグネチャを前記他の隣接中継装置に送信することを特徴とする。

【００２０】

また、請求項１３に係る発明は、上記の発明において、前記シグネチャ送信手順は、全ての隣接中継装置のなかから前記シグネチャを送信した隣接中継装置を除いた他の隣接中継装置に対して前記シグネチャを送信することを特徴とする。

【発明の効果】

【００２１】

請求項１、５、６または１０の発明によれば、隣接中継装置から受信したシグネチャの条件を満たすパケットを監視して攻撃の有無を判定し、攻撃有りと判定した場合に初めてシグネチャを隣接中継装置に送信するので、ネットワーク上の全ての中継装置に容疑シグネチャが送信される事態はなくなり、ネットワーク上にある各中継装置の処理負荷を低減し、パケットの規制に関する処理を効率良く行うことが可能になる。

【００２２】

また、請求項２、７または１１の発明によれば、隣接中継装置から受信したシグネチャの条件を満たす単位時間内のパケット数が所定の閾値を超過した場合に攻撃有りと判定す

るので、攻撃の有無を客観的かつ確実に判定することが可能になる。

【００２３】

また、請求項３、８または１２の発明によれば、シグネチャの条件を満たす単位時間内のパケット数が所定の閾値を超過した場合に直ちに攻撃有りと判定するのではなく、所定の閾値を連続して超過した回数が所定値を超過した場合に初めて攻撃有りと判定するので、攻撃の有無をより確実に判定することが可能になる。

【００２４】

また、請求項４、９または１３の発明によれば、自己にシグネチャを送信した隣接中継装置を除いた他の隣接中継装置にシグネチャを送信するので、既にパケットの規制に関する処理を行っている中継装置に対するシグネチャの送信が防止され、ネットワーク上にある各中継装置の処理負荷を低減し、パケットの規制に関する処理を効率良く行うことが可能になる。

【発明を実施するための最良の形態】

【００２５】

以下に添付図面を参照して、この発明に係る中継装置、中継方法および中継プログラム並びにネットワーク攻撃防御システムの実施例を詳細に説明する。なお、以下では、本実施例で用いる主要な用語、ネットワーク攻撃防御システムの概要および特徴、中継装置の構成および処理、本実施例の効果を順に説明し、最後に本実施例に対する種々の変形例を説明する。

【実施例】

【００２６】

[用語の説明]

まず最初に、本実施例で用いる主要な用語を説明する。本実施例で用いる「容疑シグネチャ」とは、攻撃容疑のあるパケット（攻撃容疑パケット）を制限するためのシグネチャであり、具体的には、通過が制限される攻撃容疑パケットの特徴を示す属性（例えば、宛先ＩＰアドレス、プロトコル、宛先ポート番号など）や制限内容（例えば、特定のパケットが流入するときの帯域を制限するための制限情報など）を規定して構成される。

【００２７】

また、本実施例で用いる「正規シグネチャ」とは、容疑シグネチャに該当するパケットのなかから攻撃とはみなされない正規パケット（正規ユーザの通信パケットである正規パケット）の通過を許可するためのシグネチャであり、具体的には、通過が許可される正規パケットの特徴を示す属性（例えば、送信元ＩＰアドレス、サービスタイプ、宛先ＩＰアドレス、プロトコル、宛先ポート番号など）を規定して構成される。

【００２８】

また、本実施例で用いる「不正シグネチャ」とは、不正トラヒックに含まれる不正パケット（不正トラヒック条件を満たすパケット）を制限するためのシグネチャであり、具体的には、不正パケットの送信元ＩＰアドレス等を規定して構成される。

【００２９】

[システムの概要および特徴]

次に、図１を用いて、本実施例に係るネットワーク攻撃防御システムの概要および特徴を説明する。図１は、本実施例に係るネットワーク攻撃防御システムの構成を示すシステム構成図である。

【００３０】

同図に示すように、このネットワーク攻撃防御システム１００は、ネットワーク上に複数の中継装置１０を備えて構成される。また、このネットワーク上には、ＤｏＳ攻撃やＤＤｏＳ攻撃の対象となるコンピュータとしてのサーバ２０や、かかるＤｏＳ攻撃やＤＤｏＳ攻撃を行い得るコンピュータとしての通信端末３０が接続されている。なお、以下では、図示した中継装置１０の各々を区別する場合には、それぞれ中継装置１０－１～中継装置１０－７として説明し、サーバ２０の各々を区別する場合には、サーバ２０－１またはサーバ２０－２として説明し、通信端末３０の各々を区別する場合には、通信端末３０－

１～通信端末３０－５として説明する。

【００３１】

かかるネットワーク攻撃防御システム１００において、中継装置１０は、通信端末３０のうち少なくとも１つ以上の通信端末３０がネットワーク上のサーバ２０に対してＤｏＳ攻撃またはＤＤｏＳ攻撃を行っていることを検出した場合に、パケットの通過を制御するためのシグネチャ（容疑シグネチャや不正シグネチャ）を生成するとともに、パケットの通過を許可するための正規シグネチャを生成する。そして、中継装置１０は、自ら生成したシグネチャ（容疑シグネチャ、不正シグネチャおよび正規シグネチャ）をシグネチャリストに登録する。

【００３２】

また、中継装置１０は、生成した容疑シグネチャ（さらには、正規シグネチャの生成に用いた正規条件）を隣接中継装置に送信する。その一方で、中継装置１０は、隣接中継装置から容疑シグネチャ等を受信した場合には、正規条件に基づいて正規シグネチャを生成するとともに、受信した容疑シグネチャおよび生成した正規シグネチャをシグネチャリストに登録し、さらに、隣接中継装置から受信したシグネチャ等を他の隣接中継装置に送信する。なお、隣接中継装置について例を挙げると、図１において、中継装置１０－３における隣接中継装置は、中継装置１０－１、中継装置１０－２、中継装置１０－４および中継装置１０－７であり、中継装置１０－５および中継装置１０－６とは、隣接関係をもたない。また、この隣接関係は、物理的な隣接を意味するものではない。

【００３３】

そして、中継装置１０は、上記のようにしてシグネチャリストに登録されたシグネチャに基づいてパケットの通過を制御する。つまり、不正シグネチャや容疑シグネチャに該当するパケットについては、伝送帯域を制限して通過させるかもしくは廃棄し、正規シグネチャに該当するパケットやいずれのシグネチャにも該当しないパケットについては、伝送帯域を制限せずに通過を許可する。

【００３４】

なお、中継装置１０は、攻撃を防御しながらパケットを中継するための装置であり、例えば、ルータとして機能してもよく、または、ブリッジとして機能してもよい。また、中継装置１０は、中継装置１０等を管理するための管理用ネットワークに接続されていてもよく、シグネチャは、管理用ネットワークを介して送受されてもよい。

【００３５】

このように、中継装置１０は、パケットの通過を制御するためのシグネチャ等を自ら生成してパケットを制御するだけでなく、生成したシグネチャを隣接中継装置に送信する。さらに、中継装置１０は、隣接中継装置からシグネチャを受信した場合には、かかるシグネチャに基づいてパケットを制御するとともに、他の隣接中継装置にもシグネチャを送信する。そして、本実施例における中継装置１０は、隣接中継装置から受信したシグネチャを他の隣接中継装置に送信する処理に主たる特徴があり、隣接中継装置から受信したシグネチャの条件を満たすパケットを監視して攻撃の有無を判定し、攻撃有りと判定した場合に初めてシグネチャを隣接中継装置に送信するようにしている。

【００３６】

この主たる特徴について図１を用いて簡単に説明する。図１に示すように、例えば、通信端末３０－４および通信端末３０－５がサーバ２０－１に対するＤｏＳ攻撃を行っており、中継装置１０－１が容疑のかかる攻撃を検出したとすると、中継装置１０－１は、攻撃容疑パケットを制限するための容疑シグネチャを生成し、生成した容疑シグネチャに基づいてパケットを処理するとともに、容疑シグネチャ（さらには正規条件）を隣接中継装置となる中継装置１０－３に送信する（図１の（１）および（２）参照）。

【００３７】

一方、中継装置１０－３は、中継装置１０－１から送信された容疑シグネチャを受信し、受信した容疑シグネチャに基づいてパケットを処理するとともに、受信した容疑シグネチャの条件を満たすパケットの数が単位時間内に所定の閾値を超過したか否かを判定する

（図１の（３）参照）。すなわち、かかる容疑シグネチャに該当する攻撃が中継装置１０－３を経由して行われているか否か、攻撃の有無を判定する。

【００３８】

そして、かかる判定において、容疑シグネチャの条件を満たすパケットの数が単位時間内に所定の閾値を超過した場合には、中継装置１０－３は、中継装置１０－１から受信した容疑シグネチャを隣接中継装置に送信する（図１の（４）参照）。ここで、中継装置１０－３が容疑シグネチャを送信する隣接中継装置は、容疑シグネチャを自己（中継装置１０－３）に送信した隣接中継装置（中継装置１０－１）を除く隣接中継装置、すなわち、中継装置１０－２、中継装置１０－４および中継装置１０－７である。また、図１に示す例では、通信端末３０－４および通信端末３０－５がサーバ２０－１に対する攻撃を行っているので、中継装置１０－３では「攻撃有り」と判定される。

【００３９】

さらに、中継装置１０－４および中継装置１０－２は、中継装置１０－３から送信された容疑シグネチャを受信し、受信した容疑シグネチャに基づいてパケットを処理するとともに、上記と同様、かかる容疑シグネチャに該当する攻撃が各中継装置を経由して行われているか否か判定する（図１の（５）および（６）参照）。ここで、図１に示す例では、通信端末３０－４および通信端末３０－５がサーバ２０－１に対する攻撃を行っているので、中継装置１０－２および中継装置１０－４では、受信した容疑シグネチャの条件を満たすパケットの数が単位時間内に所定の閾値を超過したと判定されず（つまり「攻撃無し」と判定され）、その結果、容疑シグネチャを隣接中継装置に送信することはしない。

【００４０】

一方、中継装置１０－７は、上記した中継装置１０－４および中継装置１０－２と同様、中継装置１０－３から送信された容疑シグネチャを受信し、受信した容疑シグネチャに基づいてパケットを処理するとともに、かかる容疑シグネチャに該当する攻撃が各中継装置を経由して行われているか否か判定するが、容疑シグネチャを自己に送信した隣接中継装置を除く隣接中継装置が存在しないため、容疑シグネチャを隣接中継装置に送信することはしない（図１の（７）参照）。

【００４１】

以上のように、ネットワーク攻撃防御システム１００において、複数の中継装置１０のうち、中継装置１０－１、中継装置１０－３および中継装置１０－７が、通信端末３０－４および通信端末３０－５から送信されるパケットを容疑シグネチャに基づいて制限しながら中継する。言い換えれば、ネットワーク攻撃防御システム１００の中継装置１０のうち、中継装置１０－５および中継装置１０－６には容疑シグネチャが送信されない（全ての中継装置１０に容疑シグネチャが送信されるわけではない）。このため、容疑のかかる攻撃を検出したとき等の各中継装置１０にかかる処理負荷を低減することが可能になる。

【００４２】

なお、中継装置１０が送信するシグネチャは、容疑シグネチャだけに限定されず、中継装置１０が他のシグネチャを送信するようにしてもよく、また、容疑シグネチャに加えて他のシグネチャを送信するようにしてもよい。

【００４３】

[中継装置の構成]

次に、図２を用いて、図１に示した中継装置１０の構成を説明する。図２は、中継装置１０の構成を示すブロック図である。同図に示すように、この中継装置１０は、ネットワークインタフェース部１１と、パケット取得部１２と、攻撃検出部１３（並びに攻撃容疑検出条件テーブル１３ａ、不正トラヒック検出条件テーブル１３ｂおよび正規条件テーブル１３ｃ）と、シグネチャ通信部１４と、パケット数判定部１５ａと、連続超過回数判定部１５ｂと、フィルタ部１６（並びにシグネチャリスト１６ａ）とを備えて構成される。

【００４４】

また、中継装置１０は、ＣＰＵ（Central Processing Unit）やメモリ、ハードディスク等を有しており、パケット取得部１２、攻撃検出部１３、シグネチャ通信部１４、パケ

ット数判定部１５ａ、連続超過回数判定部１５ｂおよびフィルタ部１６は、ＣＰＵによって処理されるプログラムのモジュールであってもよい。また、このプログラムのモジュールは、１つのＣＰＵで処理されてもよく、複数のＣＰＵに分散して処理されてもよい。さらに、中継装置１０には、Ｌｉｎｕｘ等の汎用ＯＳをインストールしておき、汎用ＯＳに具備されるパケットフィルタをフィルタ部１６として機能させてもよい。

【００４５】

なお、シグネチャ通信部１４は特許請求の範囲に記載の「シグネチャ送信手段」に対応し、パケット数判定部１５ａは同じく「攻撃有無判定手段」および「パケット数判定手段」に対応し、連続超過回数判定部１５ｂは同じく「攻撃有無判定手段」および「連続超過回数判定」に対応する。

【００４６】

図２において、ネットワークインタフェース部１１は、ネットワークと接続されている通信機器との間でパケットを送受する手段であり、具体的には、ＬＡＮ（Local Area Network）またはＷＡＮ（Wide Area Network）などのネットワークと接続するためのネットワーク接続カード等によって構成される。なお、図２には示していないが、キーボードやマウス、マイクなど、ネットワーク管理者から各種の情報や指示の入力を受付ける入力手段や、モニタ（若しくはディスプレイ、タッチパネル）やスピーカなど、各種の情報を出力する出力手段を備えて中継装置１０を構成するようにしてもよい。

【００４７】

パケット取得部１２は、ネットワークインタフェース部１１が受信したパケットを取得し、取得したパケットの統計に関する統計情報を攻撃検出部１３およびパケット数判定部１５ａに提供する処理部である。

【００４８】

攻撃検出部１３は、パケット取得部１２によって提供された統計情報に基づいて、攻撃の検出および攻撃の分析を行う処理部であり、図２に図示するように、攻撃容疑検出条件テーブル１３ａ、不正トラヒック検出条件テーブル１３ｂおよび正規条件テーブル１３ｃにそれぞれ接続される。ここで、各テーブル１３ａ～１３ｃに記憶される情報を具体的に説明した後に、攻撃検出部１３による処理内容を説明する。

【００４９】

図３は、攻撃容疑検出条件テーブル１３ａに記憶される情報、より詳細には、受信パケットが攻撃パケットである可能性がある攻撃容疑パケットを検出するために使用される「攻撃容疑検出条件」の一例を示す図である。同図に示すように、攻撃容疑検出条件は、検出属性、検出閾値および検出間隔の組合せからなる複数組（ここでは３組）のレコードで構成され、かかる攻撃容疑検出条件の各レコードの内のいずれかのレコードの条件にトラヒックが一致した場合に、このトラヒックの通信パケットは攻撃容疑パケットであると認識される。なお、番号はレコードを特定するために便宜上使用されるものである。

【００５０】

攻撃容疑検出条件の「検出属性」には、例えば、ＩＰパケットに含まれるＩＰヘッダ部の属性や、ＩＰパケットのペイロード部に含まれるＴＣＰヘッダ部またはＵＤＰヘッダ部の属性が指定される。具体的には、図３において、番号１のレコードの検出属性は、「Destination IP Address（宛先ＩＰアドレス）」が「192.168.1.1/32」であり（dst=192.168.1.1/32）、ＩＰの上位層（ＴＣＰまたはＵＤＰ）のプロトコル種別を示す「Protocol（プロトコル）」が「ＴＣＰ」であり（Protocol=TCP）、かつ、ＩＰの上位層プロトコルがどのアプリケーションの情報であるかを示す「Destination Port（宛先ポート番号）」が「８０」である（Port=80）という属性値の組で指定される。

【００５１】

また、番号２のレコード検出属性は、「Destination IP Address（宛先ＩＰアドレス）」が「192.168.1.2/32」であり（dst=192.168.1.2/32）、かつ、「Protocol（プロトコル）」が「ＵＤＰ（User Datagram protocol）」である（Protocol=UDP）という属性値の組で指定される。同様に、番号３のレコード検出属性は、「Destination IP Address（宛先

ＩＰアドレス）」が「192.168.1.0/24」という属性で指定される。

【００５２】

攻撃容疑検出条件の「検出閾値」は、同じレコードで指定される検出属性を持つ受信パケットのトラヒックを攻撃容疑トラヒックとして検出するための最低の伝送帯域を指定したものであり、攻撃容疑検出条件の「検出間隔」は、同じく最低の連続時間を指定したものである。なお、図３には示していないが、検出属性においては、「Destination IP Address（宛先ＩＰアドレス）」の値を無条件（ａｎｙ）とし、かつ、ＩＰの上位層のプロトコル種別を示す「Protocol（プロトコル）」が「ＩＣＭＰ（Internet Control Message Protocol）」となる属性値の組を指定するようにしてもよい。

【００５３】

図４は、不正トラヒック検出条件テーブル１３ｂに記憶される情報、より詳細には、攻撃容疑パケットのトラヒックから不正トラヒックを検出するために用いられる「不正トラヒック条件」の一例を示す図である。同図に示すように、不正トラヒック条件は、既知のＤＤｏＳ攻撃の複数のトラヒックパターンから構成され、攻撃容疑パケットのトラヒックがいずれかのトラヒックパターンに合致した場合に、不正トラヒックであると認識される。なお、番号はレコード（パターン）を特定するために便宜上使用されるものである。

【００５４】

具体的には、番号１の不正トラヒック条件は、「伝送帯域Ｔ１Ｋｂｐｓ以上、パケットがＳ１秒以上連続送信されている」というトラヒックパターンを示している。また、番号２の不正トラヒック条件は、「伝送帯域Ｔ２Ｋｂｐｓ以上、ＩＣＭＰ（Internet Control Message Protocol）上のエコー応答（Echo Reply）メッセージのパケットがＳ２秒以上連続送信されている」というトラヒックパターンを示している。さらに、番号３の不正トラヒック条件は、「伝送帯域Ｔ３Ｋｂｐｓ以上、データが長すぎるためパケットに含まれるデータは複数ＩＰパケットに分割して送信していることを示すフラグメントパケットがＳ３秒以上連続送信されている」というトラヒックパターンを示している。

【００５５】

図５は、正規条件テーブル１３ｃに記憶される情報、より詳細には、正当な利用者が利用している通信端末３０から送信されるパケットを表す「正規条件」の一例を示す図である。同図に示すように、正規条件は、ＩＰパケットにおける属性とそれら属性値の組からなる複数のレコードで構成される。なお、番号はレコード（パターン）を特定するために便宜上使用されるものである。

【００５６】

具体的には、番号１のレコードの検出属性は、ＩＰの「Source IP Address（送信元ＩＰアドレス）」が「172.16.10.0/24」であることを指定し（src=172.16.10.0/24）、番号２のレコードの検出属性はＩＰ上のサービス品質を示す「Type of Service（サービスタイプ）」が「（１６進で）０１」であることを指定している（TOS=0x01）。このような正規条件には、例えば、サーバ所有者の会社の支店や、関連会社など、防御対象のサーバ２０等の送信元ＩＰアドレスが設定され、サーバ２０が収容されているＬＡＮの所有者が正規ユーザであると認識しているネットワークの送信元ＩＰアドレスなどが設定される。

【００５７】

図２の説明に戻ると、攻撃検出部１３は、パケット取得部１２によって提供された統計情報に基づいて攻撃の検出を検出した場合に、攻撃容疑トラヒックの通信パケット（攻撃容疑パケット）を制限するための容疑シグネチャを生成する。具体的には、攻撃検出部１３は、図３に示した攻撃容疑検出条件に従って、検出間隔で指定されているより長い時間連続して、検出閾値で指定されている以上の伝送帯域を使用している、検出属性に合致するトラヒックをチェックし、各レコードの内のいずれかのレコードに合致した場合には、このトラヒックを攻撃容疑トラヒックとして検出し、このときに検出された攻撃容疑トラヒックが満たしている攻撃容疑検出条件のレコードの検出属性を容疑シグネチャとして生成する。

【００５８】

また、攻撃検出部１３は、攻撃を検出した場合に、容疑シグネチャとともに正規シグネチャを生成する。具体的には、図５に示した正規条件を参照し、正規条件の全てのレコード毎に、容疑シグネチャとのＡＮＤ条件をとり、これを正規シグネチャとして生成する。この正規シグネチャは、容疑シグネチャから正規ユーザの通信パケットである正規パケットを許可するために用いられるシグネチャであるが、例えば、図３および図５の例を用いて説明すると、図３における番号１のレコードの条件で検出されるパケットの容疑シグネチャは、[dst=192.168.1.1/32，Protocol=TCP，Port=80]となり、図５において、正規シグネチャは、[src=172.16.10.24，dst=192.168.1.1/32，Protocol=TCP，Port=80]および[TOS=0x01，dst=192.168.1.1/32，Protocol=TCP，Port=80]となる。

【００５９】

さらに、攻撃検出部１３は、図４に示した不正トラヒック条件のいずれかのパターンに合致するトラヒックを検出した場合に、不正トラヒックを制限するための不正シグネチャを生成する。具体的には、検出された不正トラヒック条件を満たすパケットの送信元ＩＰアドレスを不正アドレス範囲として特定し、この不正アドレス範囲であり、かつ、容疑シグネチャに合致するという条件を不正シグネチャとして生成する。

【００６０】

上述してきた攻撃検出部１３によって生成された容疑シグネチャ、正規シグネチャおよび不正シグネチャは、シグネチャリスト１６ａに登録される。なお、シグネチャリスト１６ａに登録されるシグネチャ（容疑シグネチャ、正規シグネチャおよび不正シグネチャ）としては、かかる攻撃検出部１３によって生成されたシグネチャの他に、後述するシグネチャ通信部１４を介して隣接中継装置から受信したシグネチャもある。

【００６１】

図２において、シグネチャ通信部１４は、攻撃検出部１３が生成したシグネチャ等を隣接中継装置に送信するとともに、隣接中継装置から送信されたシグネチャを受信し、さらに、隣接中継装置から受信したシグネチャを他の隣接中継装置に送信する処理部である。ここで、隣接中継装置から受信したシグネチャを他の隣接中継装置に送信する処理は、後述するパケット数判定部１５ａおよび連続超過回数判定部１５ｂによる判定結果に従って実行される。

【００６２】

パケット数判定部１５ａは、シグネチャ通信部１４によって受信されたシグネチャの条件を満たす単位時間内のパケット数が所定の閾値を超過したか否かを判定する処理部である。具体的には、パケット数判定部１５ａは、パケット取得部１２によって提供された統計情報から、シグネチャの条件を満たすパケットを単位時間毎に取得し、取得したパケットの数が所定の閾値を超過したか否かを判定する。

【００６３】

連続超過回数判定部１５ｂは、パケット数判定部１５ａが所定の閾値を超過したと判定した場合に、所定の閾値を連続して超過した回数が所定値を超過したか否かを判定する処理部である。そして、連続超過回数判定部１５ｂは、所定の閾値を連続して超過した回数が所定値を超過した場合には、シグネチャ送信部１４に対して、隣接中継装置から受信したシグネチャを他の隣接中継装置に送信するように指示を出力する。なお、かかる指示を受けたシグネチャ送信部１４は、シグネチャを自己に送信した隣接中継装置を除く隣接中継装置を選択し、選択した隣接中継装置に対してシグネチャを送信する。

【００６４】

図２において、フィルタ部１６は、ネットワークインタフェース部１１が受信したパケットを受け入れて、シグネチャリスト１６ａに基づいてパケットの通過（ネットワークインタフェース部１１からのパケットの出力）を制御する処理部である。具体的には、入力されたパケットについて、シグネチャリスト１６ａに登録された「不正シグネチャ」、「正規シグネチャ」、「容疑シグネチャ」のいずれかに該当するか（もしくはいずれにも該当しないか）を判別した上で、該当するシグネチャに基づいてパケットの通過を制御する。

【００６５】
より詳細には、フィルタ部１６は、不正シグネチャに該当するパケットは、不正なパケットを処理するための不正キューに入力し、容疑シグネチャに該当するパケットは、容疑ユーザ用の容疑キューに入力し、正規シグネチャに該当するパケットまたはいずれのシグネチャにも該当しないパケットは、正規ユーザ用の正規キューに入力する。その上で、フィルタ部１６は、正規キューに入力されたパケットについては、伝送帯域を制限せずにネットワークインタフェース部１１から出力し、容疑キューおよび不正キューに入力されたパケットについては、それぞれのシグネチャ（条件を満たすとして選択されたシグネチャ）が示す伝送帯域制限値に従って制限して出力する。
【００６６】
なお、フィルタ部１６は、シグネチャリスト１６ａに登録されたシグネチャの検出属性等が所定の解除判断基準を満たした場合には、この所定の解除判断基準を満たしたシグネチャを解除し、解除したシグネチャに基づいてパケットの通過を制御する処理を停止する。
【００６７】
[攻撃容疑パケット検出時の処理]
続いて、図６を参照して、上記した中継装置１０による攻撃容疑パケット検出時の動作処理を説明する。図６は、攻撃容疑パケット検出時の処理手順を示すフローチャートである。
【００６８】
同図に示すように、中継装置１０の攻撃検出部１３は、図３に示した攻撃容疑検出条件テーブル１３ａに基づいて攻撃容疑トラヒックを検出すると（ステップＳ１）、容疑シグネチャおよび正規シグネチャを生成する（ステップＳ２）。
【００６９】
そして、攻撃検出部１３は、生成した容疑シグネチャおよび正規シグネチャをフィルタ部１６のシグネチャリスト１６ａに登録する（ステップＳ３）。さらに、シグネチャ通信部１４は、攻撃検出部１３が生成したシグネチャ等（本実施例では、容疑シグネチャおよび正規条件）を隣接中継装置に送信する（ステップＳ４）。
【００７０】
[シグネチャ受信時の処理]
続いて、図７を参照して、上記した中継装置１０によるシグネチャ受信時の動作処理を説明する。図７は、シグネチャ受信時の処理手順を示すフローチャートである。
【００７１】
同図に示すように、中継装置１０のシグネチャ通信部１４が、隣接中継装置から送信されたシグネチャ等（本実施例では、容疑シグネチャおよび正規条件）を受信すると（ステップＳ１１）、攻撃検出部１３は、シグネチャ通信部１４が受信した正規条件に基づいて正規シグネチャを生成する（ステップＳ１２）。
【００７２】
さらに、攻撃検出部１３は、隣接中継装置から受信した容疑シグネチャおよび上記で生成した正規シグネチャをフィルタ部１６のシグネチャリスト１６ａに登録する（ステップＳ１３）。その後、パケット数判定部１５ａは、パケット取得部１２によって提供された統計情報から、上記でシグネチャリスト１６ａに登録した容疑シグネチャの条件を満たすパケットを単位時間毎に取得し、取得したパケットの数が所定の閾値を超過したか否かを判定する（ステップＳ１４）。
【００７３】
ここで、かかる所定の閾値を超過した場合（ステップＳ１４肯定）、連続超過回数判定部１５ｂは、所定の閾値を連続して超過した回数が、所定値を超過したか否かを判定する（ステップＳ１５）。その結果、かかる所定の閾値を連続して超過した回数が所定値を超過した場合（ステップＳ１５肯定）、シグネチャ送信部１４は、上記で受信した容疑シグネチャおよび正規条件を隣接中継装置に送信する（ステップＳ１６）。つまり、シグネチ

ャを自己に送信した隣接中継装置を除く隣接中継装置を選択し、選択した隣接中継装置に対してシグネチャを送信する。

【００７４】

なお、上記したステップＳ１４において、パケットの数が所定の閾値を超過しなかった場合（ステップＳ１４否定）や、上記したステップＳ１５において、所定の閾値を連続して超過した回数が所定値を超過しなかった場合（ステップＳ１５否定）には、隣接中継装置から受信したシグネチャを他の隣接中継装置に送信する処理（上記のステップＳ１６の処理）は行われない。

【００７５】

［不正パケット検出時の処理］

続いて、図８を参照して、上記した中継装置１０による不正パケット検出時の動作処理を説明する。図８は、不正パケット検出時の処理手順を示すフローチャートである。

【００７６】

同図に示すように、中継装置１０の攻撃検出部１３が、図４に示した不正トラヒック条件検出テーブル１３ｂ等に基づいて不正トラヒックを検出すると（ステップＳ２１）、不正シグネチャを生成する（ステップＳ２２）。そして、攻撃検出部１３は、生成した不正シグネチャをフィルタ部１６のシグネチャリスト１６ａに登録する（ステップＳ２３）。

【００７７】

［パケット制御時の処理］

続いて、図９を参照して、上記した中継装置１０によるパケット制御時の動作処理を説明する。図９は、パケット制御時の処理手順を示すフローチャートである。

【００７８】

同図に示すように、フィルタ部１６は、ネットワークインタフェース部１１からパケットが入力されると、シグネチャリスト１６ａに登録された不正シグネチャに合致するか否かを判断する（ステップＳ３１）。そして、不正シグネチャに合致した場合には（ステップＳ３１肯定）、フィルタ部１６は、不正なパケットを処理するための不正キューにパケットを入力する（ステップＳ３２）。

【００７９】

これとは反対に、不正シグネチャに合致しない場合には（ステップＳ３１否定）、フィルタ部１６は、入力されたパケットが、シグネチャリスト１６ａに登録された正規シグネチャに合致するか否かを判断する（ステップＳ３３）。そして、正規シグネチャに合致した場合には（ステップＳ３３肯定）、フィルタ部１６は、正規なユーザ用の正規キューにパケットを入力する（ステップＳ３４）。

【００８０】

さらに、この正規シグネチャにも合致しない場合には（ステップＳ３３否定）、フィルタ部１６は、入力されたパケットが、シグネチャリスト１６ａに登録された容疑シグネチャに合致するか否かを判断する（ステップＳ３５）。そして、容疑シグネチャに合致した場合には（ステップＳ３５肯定）、フィルタ部１６は、容疑ユーザ用の容疑キューにパケットを入力する（ステップＳ３６）。これとは反対に、容疑シグネチャに合致しない場合には（ステップＳ３５否定）、フィルタ部１６は、正規キューにパケットを入力する（ステップＳ３７）。

【００８１】

そして、フィルタ部１６は、それぞれのキューにあるパケットについて、正規キューであれば、伝送帯域を制限せずにネットワークインタフェース部１１から出力し、容疑キューおよび不正キューであれば、それぞれのシグネチャが示す伝送帯域制限値に従って制限して出力する。なお、不正シグネチャ、正規シグネチャ、容疑シグネチャの各シグネチャは、それぞれシグネチャリスト１６ａに複数登録されてもよい。また、登録されたシグネチャの検出属性等が所定の判断基準を満たした場合に、フィルタ部１６は、所定の判断基準を満たしたシグネチャを解除し、解除したシグネチャに基づいたパケットの通過を制御する処理を停止する。

【００８２】
［実施例の効果］
上述してきたように、上記の実施例によれば、隣接中継装置から受信したシグネチャの条件を満たすパケットを監視して攻撃の有無を判定し、攻撃有りと判定した場合に初めてシグネチャを隣接中継装置に送信するので、ネットワーク上の全ての中継装置１０に容疑シグネチャが送信される事態はなくなり、ネットワーク上にある各中継装置１０の処理負荷を低減し、パケットの規制に関する処理を効率良く行うことが可能になる。
【００８３】
また、上記の実施例によれば、隣接中継装置から受信したシグネチャの条件を満たす単位時間内のパケット数が所定の閾値を超過した場合に攻撃有りと判定するので、攻撃の有無を客観的かつ確実に判定することが可能になる。より詳細には、シグネチャの条件を満たす単位時間内のパケット数が所定の閾値を超過した場合に直ちに攻撃有りと判定するのではなく、所定の閾値を連続して超過した回数が所定値を超過した場合に初めて攻撃有りと判定するので、攻撃の有無をより確実に判定することが可能になる。
【００８４】
また、上記の実施例によれば、自己にシグネチャを送信した隣接中継装置を除いた他の隣接中継装置にシグネチャを送信するので、既にパケットの規制に関する処理を行っている中継装置１０に対するシグネチャの送信が防止され、ネットワーク上にある各中継装置１０の処理負荷を低減し、パケットの規制に関する処理を効率良く行うことが可能になる。
【００８５】
［他の実施例］
さて、これまで本発明の実施例について説明したが、本発明は上述した実施例以外にも、種々の異なる形態にて実施されてよいものである。
【００８６】
例えば、上記の実施例では、シグネチャの条件を満たす単位時間内のパケット数が所定の閾値を超過し、かつ、所定の閾値を連続して超過した回数が所定値を超過した場合に攻撃有りと判定する場合を説明したが、本発明はこれに限定されるものではなく、単位時間内のパケット数が所定の閾値を超過した場合に直ちに攻撃有りと判定するようにしてもよい。すなわち、上記の実施例で説明した攻撃有無の判定手法は、あくまでも一例であって、本発明はこれに限定されるものではなく、他の攻撃有無判定手法を採用する場合にも本発明を同様に適用することができる。
【００８７】
また、上記の実施例で図示した各装置（例えば、図１に例示した中継装置１０）の各構成要素は機能概念的なものであり、必ずしも物理的に図示の如く構成されていることを要しない。すなわち、中継装置１０の分散・統合の具体的形態は図示のものに限られず、中継装置１０の全部または一部を各種の負荷や使用状況などに応じて、任意の単位で機能的または物理的に分散・統合して構成することができる。さらに、中継装置１０にて行なわれる各処理機能は、その全部または任意の一部が、ＣＰＵおよび当該ＣＰＵにて解析実行されるプログラムにて実現され、あるいは、ワイヤードロジックによるハードウェアとして実現され得る。
【００８８】
また、上記の実施例で説明した各処理のうち、自動的におこなわれるものとして説明した処理の全部または一部を手動的におこなうこともでき、あるいは、手動的におこなわれるものとして説明した処理の全部または一部を公知の方法で自動的におこなうこともできる。この他、上記文書中や図面中で示した処理手順、制御手順、具体的名称、各種のデータやパラメータを含む情報（例えば、攻撃容疑検出条件テーブル、不正トラヒック検出条件テーブル、正規条件テーブルの内容等）については、特記する場合を除いて任意に変更することができる。
【００８９】

なお、上記の実施例では、本発明を実現する各装置（例えば、中継装置１０）を機能面から説明したが、各装置の各機能はパーソナルコンピュータやワークステーションなどのコンピュータにプログラムを実行させることによって実現することもできる。すなわち、本実施例１で説明した各種の処理手順は、あらかじめ用意されたプログラムをコンピュータ上で実行することによって実現することができる。そして、これらのプログラムは、インターネットなどのネットワークを介して配布することができる。さらに、これらのプログラムは、ハードディスク、フレキシブルディスク（ＦＤ）、ＣＤ－ＲＯＭ、ＭＯ、ＤＶＤなどのコンピュータで読み取り可能な記録媒体に記録され、コンピュータによって記録媒体から読み出されることによって実行することもできる。つまり、例を挙げれば、実施例に示したような中継装置用プログラムを格納したＣＤ－ＲＯＭを配布し、このＣＤ－ＲＯＭに格納されたプログラムを各コンピュータが読み出して実行するようにしてもよい。

【産業上の利用可能性】

【００９０】

以上のように、本発明に係る中継装置、中継方法および中継プログラム並びにネットワーク攻撃防御システムは、パケットの通過を制御するためのシグネチャを隣接中継装置から受信し、当該受信したシグネチャを他の隣接中継装置に送信する場合に有用であり、特に、ネットワーク上にある各中継装置の処理負荷を低減し、パケットの規制に関する処理を効率良く行うことに適する。

【図面の簡単な説明】

【００９１】

【図１】ネットワーク攻撃防御システムの構成を示すシステム構成図である。

【図２】中継装置の構成を示すブロック図である。

【図３】攻撃容疑検出条件テーブルに記憶される情報の例を示す図である。

【図４】不正トラヒック検出条件テーブルに記憶される情報の例を示す図である。

【図５】正規条件テーブルに記憶される情報の例を示す図である。

【図６】攻撃容疑パケット検出時の処理手順を示すフローチャートである。

【図７】シグネチャ受信時の処理手順を示すフローチャートである。

【図８】不正パケット検出時の処理手順を示すフローチャートである。

【図９】パケット制御時の処理手順を示すフローチャートである。

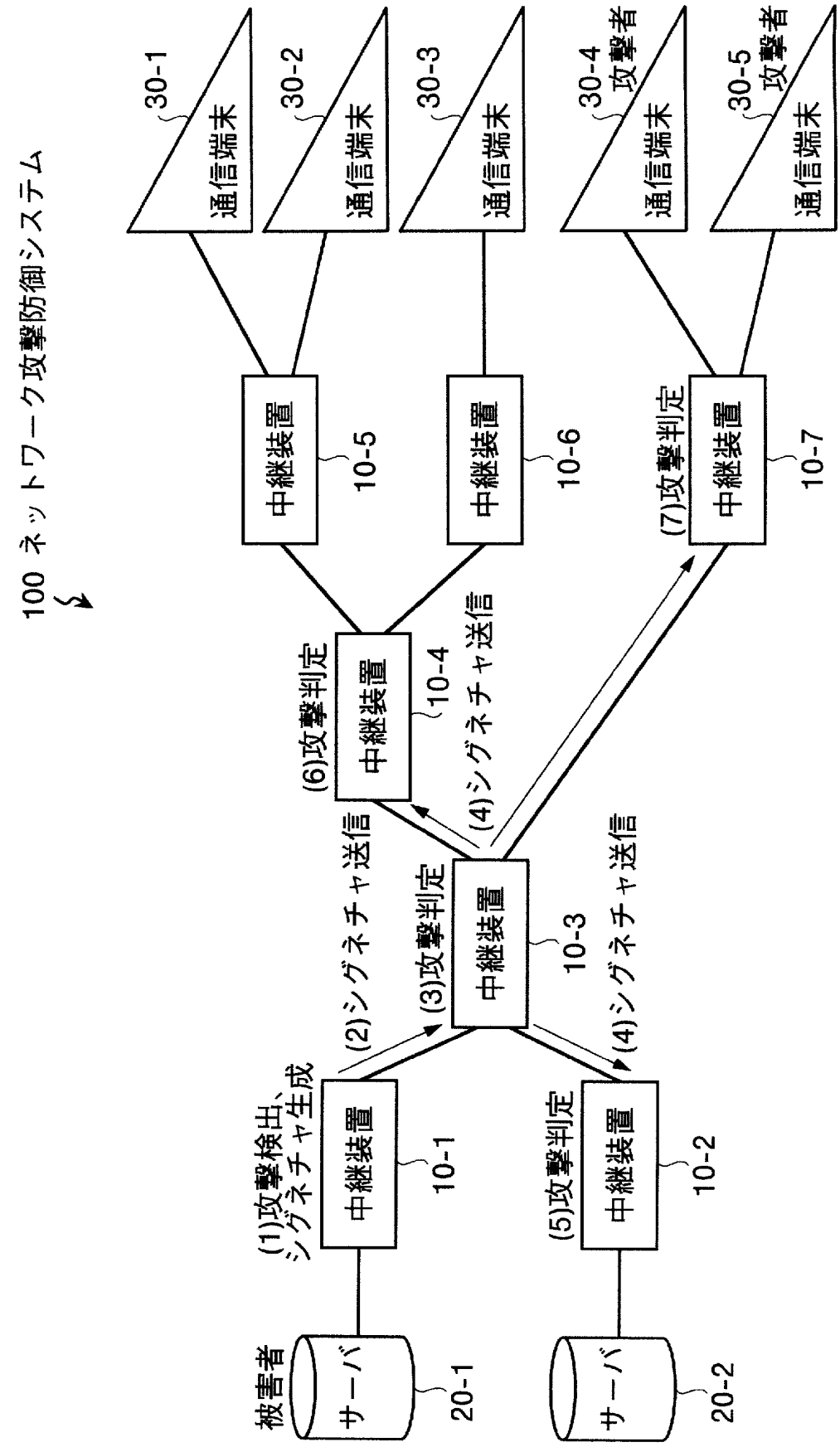
【符号の説明】

【００９２】

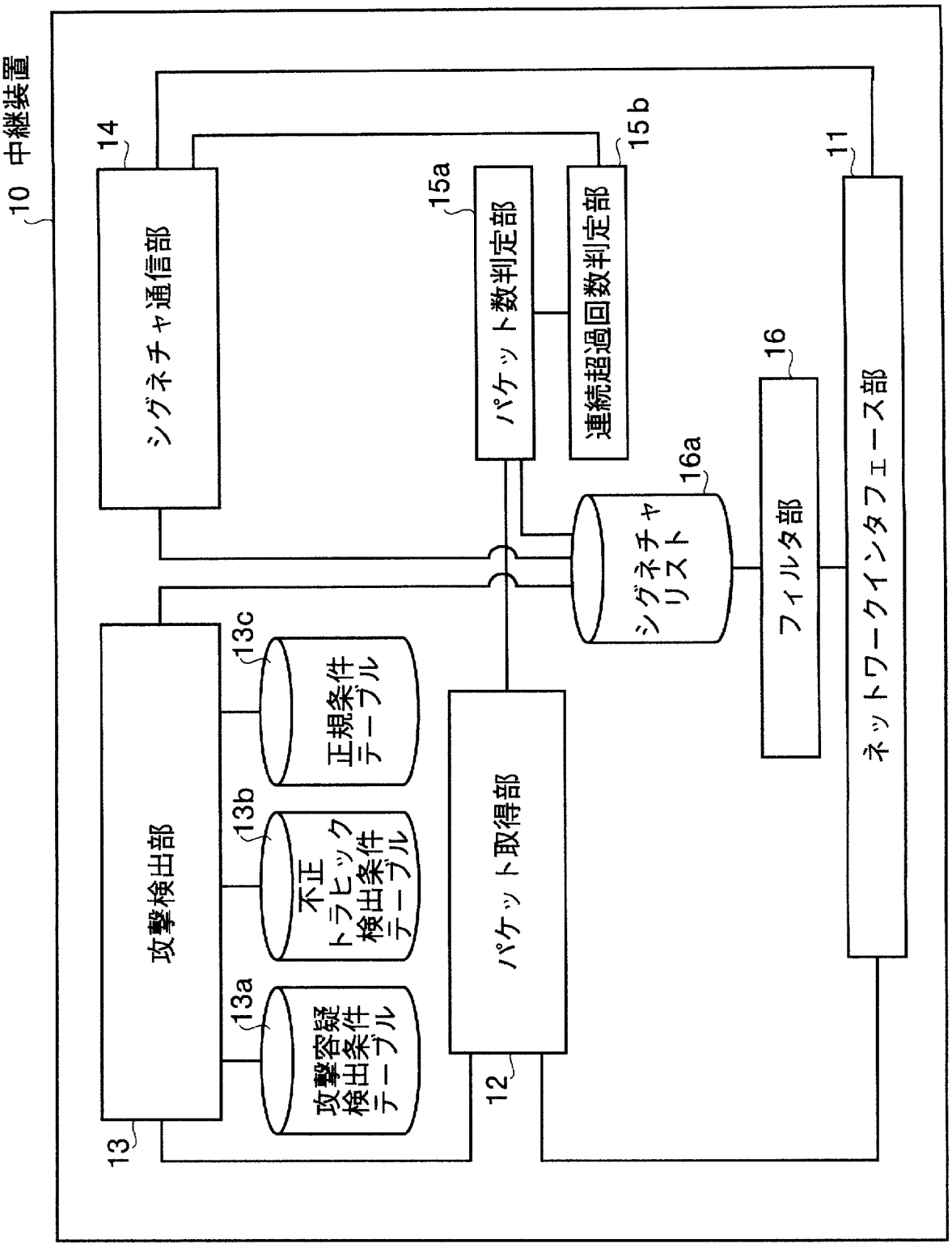
１０　中継装置
１１　ネットワークインタフェース
１２　パケット取得部
１３　攻撃検出部
１４　シグネチャ通信部（シグネチャ送信部）
１５ａ　パケット数判定部
１５ｂ　連続超過回数判定部
１６　フィルタ部
２０　サーバ
３０　通信端末
１００　ネットワーク攻撃防御システム

【書類名】図面

【図１】


100 ネットワーク攻撃防御システム
30-1 通信端末
30-2 通信端末
30-3 通信端末
30-4 攻撃者 通信端末
30-5 攻撃者 通信端末
中継装置 10-5
中継装置 10-6
中継装置 10-7
中継装置 10-4
中継装置 10-3
中継装置 10-1
中継装置 10-2
(6)攻撃判定
(4)シグネチャ送信
(7)攻撃判定
(2)シグネチャ送信
(3)攻撃判定
(4)シグネチャ送信
(1)攻撃検出、シグネチャ生成
(5)攻撃判定
被害者 サーバ 20-1
サーバ 20-2

【図２】


10 中継装置
14
シグネチャ通信部
15a
パケット数判定部
15b
連続超過回数判定部
11
16
フィルタ部
16a
シグネチャリスト
ネットワークインタフェース部
攻撃検出部
13c
正規条件テーブル
13b
不正トラヒック検出条件テーブル
13a
攻撃容疑検出条件テーブル
13
パケット取得部
12

【図３】

13a 攻撃容疑検出条件テーブル

番号	検出属性	検出閾値	検出間隔
1	{Dst=192.168.1.1/32,Protocol=TCP,Port=80}	500Kbps	10秒
2	{Dst=192.168.1.2/32,Protocol=UDP}	300Kbps	10秒
3	{Dst=192.168.1.1/24}	1000Kbps	20秒
⋮			

【図４】

13b 不正トラヒック条件検出テーブル

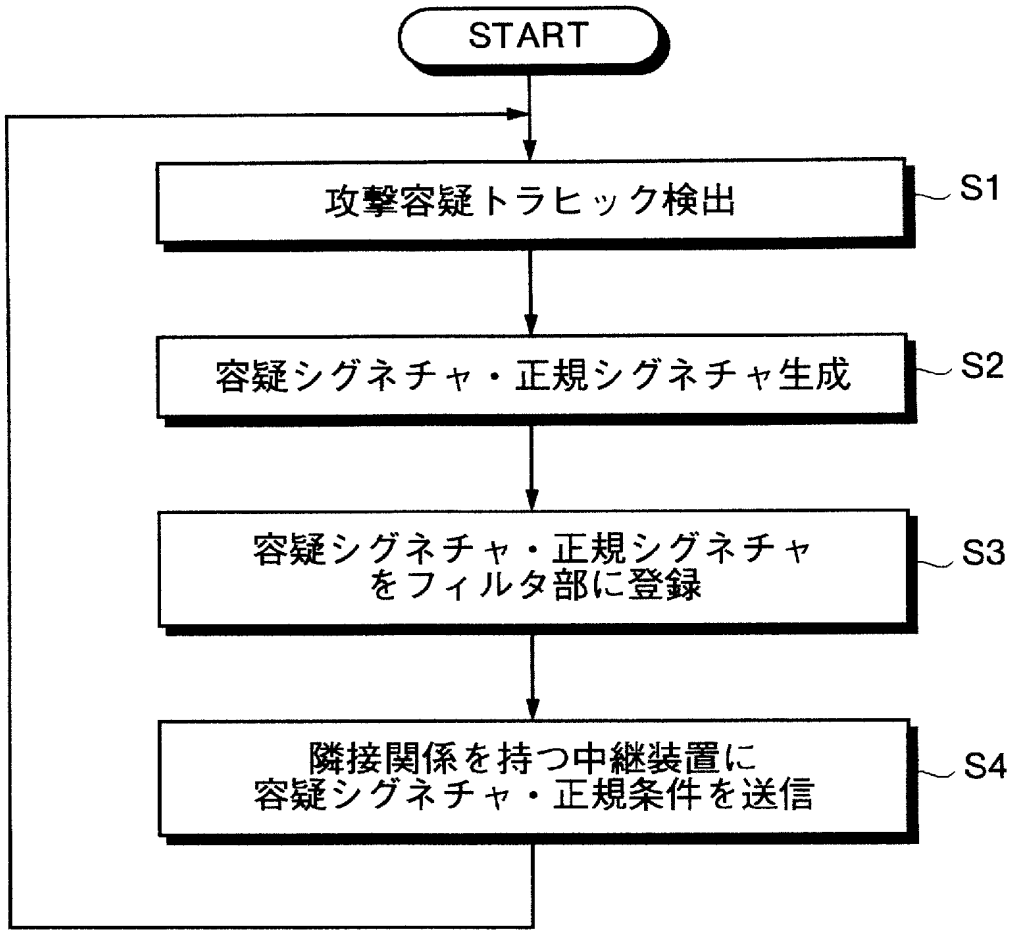
番号	不正トラヒック条件
1	T1Kbps以上のパケットがS1秒以上連続送信されている
2	T2Kbps以上のICMP/Echo Replyパケットが S2秒以上連続送信されている
3	T3Kbps以上のフラグメントパケットが S3秒以上連続送信されている
⋮	

【図５】

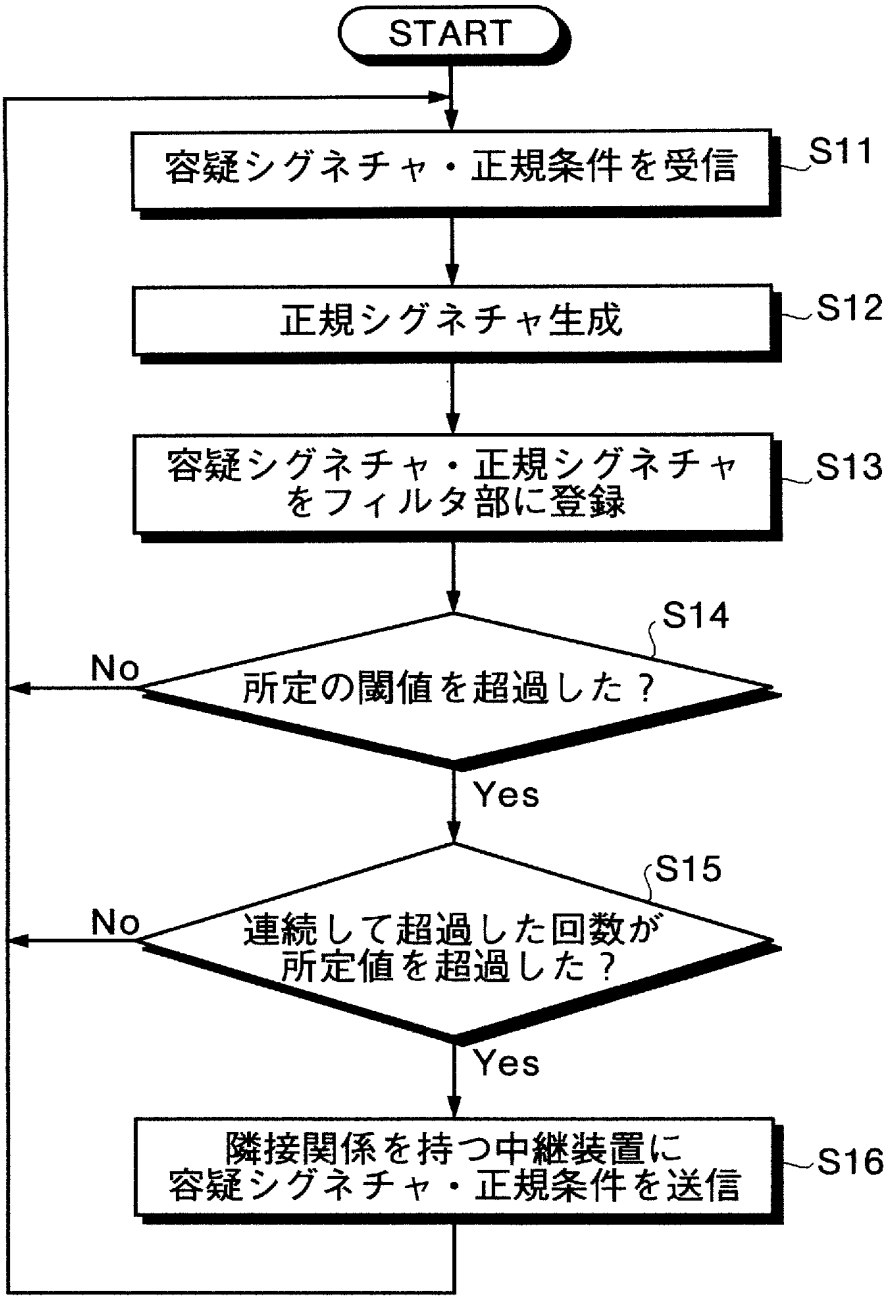
13c 正規条件テーブル

番号	検出属性
1	{Src=172.16.10.0/24}
2	{TOS=0x01}
⋮	

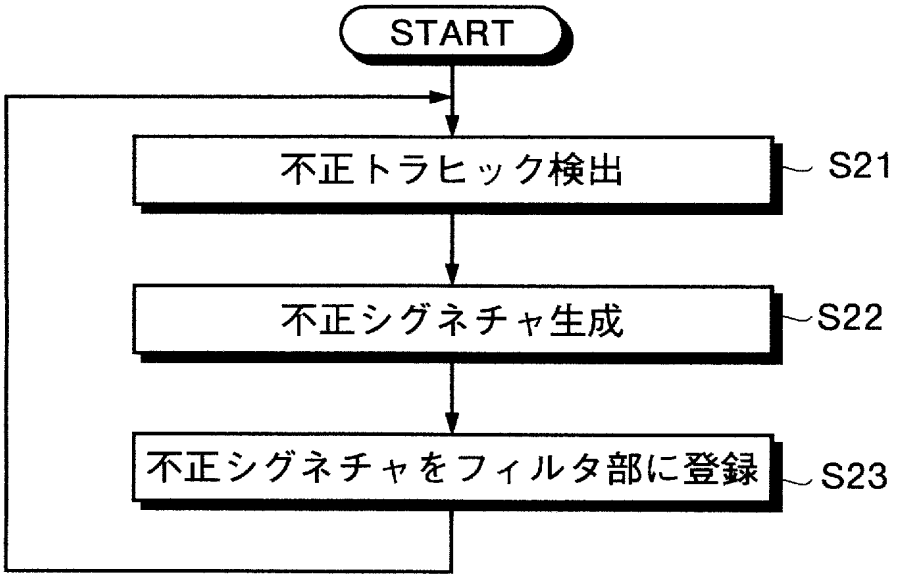
【図６】


START
攻撃容疑トラヒック検出
S1
容疑シグネチャ・正規シグネチャ生成
S2
容疑シグネチャ・正規シグネチャ
をフィルタ部に登録
S3
隣接関係を持つ中継装置に
容疑シグネチャ・正規条件を送信
S4

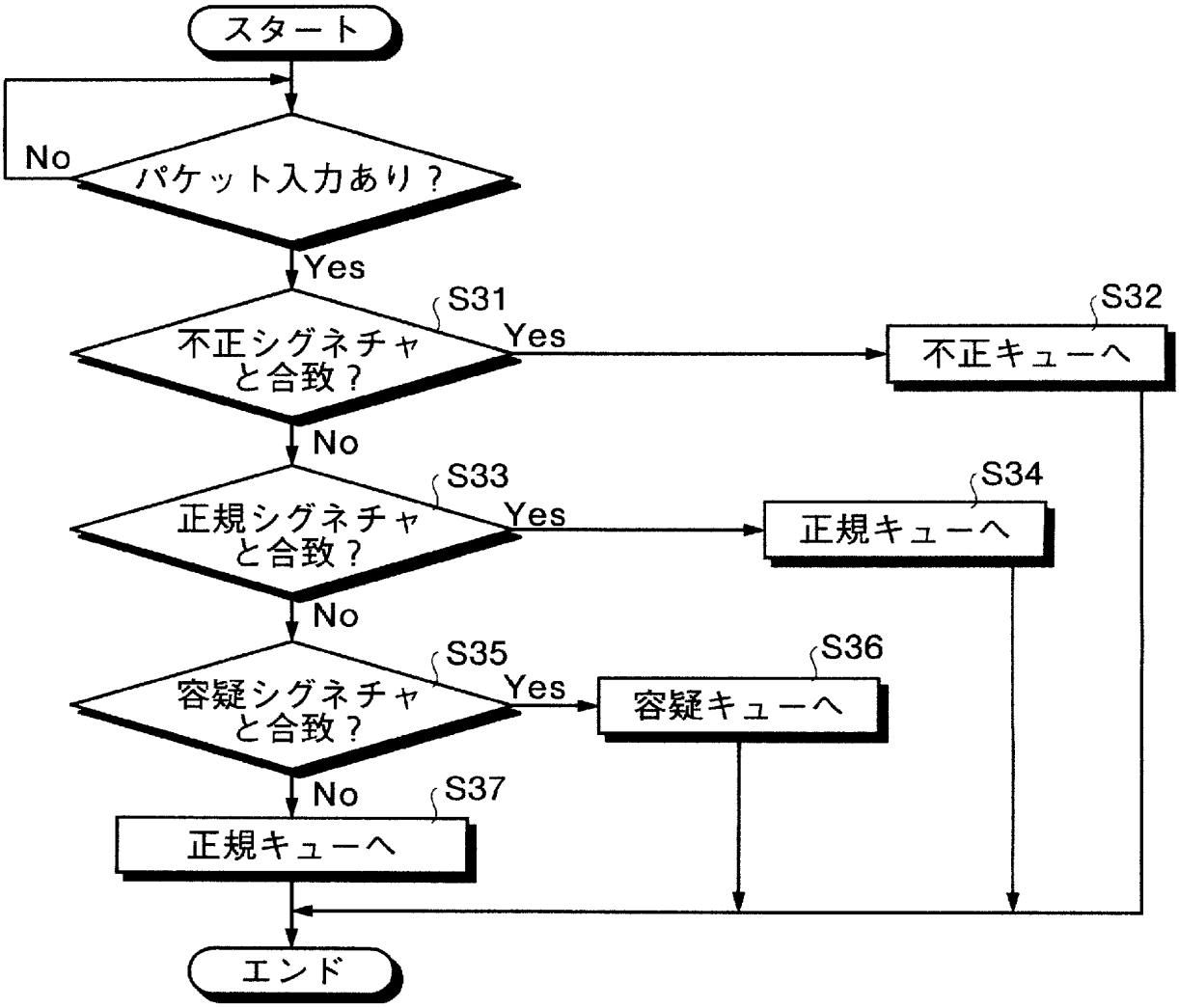
【図７】


START
容疑シグネチャ・正規条件を受信
S11
正規シグネチャ生成
S12
容疑シグネチャ・正規シグネチャ
をフィルタ部に登録
S13
S14
No
所定の閾値を超過した？
Yes
S15
No
連続して超過した回数が
所定値を超過した？
Yes
隣接関係を持つ中継装置に
容疑シグネチャ・正規条件を送信
S16

【図８】



【図９】


スタート
No
パケット入力あり？
Yes
S31
不正シグネチャと合致？
Yes
S32
不正キューへ
No
S33
正規シグネチャと合致？
Yes
S34
正規キューへ
No
S35
容疑シグネチャと合致？
Yes
S36
容疑キューへ
No
S37
正規キューへ
エンド

【書類名】要約書
【要約】
【課題】ネットワーク上にある各中継装置の処理負荷を低減し、パケットの規制に関する処理を効率良く行うことを課題とする。
【解決手段】中継装置１０は、隣接中継装置からシグネチャを受信すると、受信したシグネチャの条件を満たす単位時間内のパケット数が所定の閾値を超過したか否かを判定する。そして、中継装置１０は、単位時間内のパケット数が所定の閾値を超過したと判定された場合に、当該所定の閾値を連続して超過した回数が所定値を超過したか否かを判定する。このような判定の結果、所定の閾値を連続して超過した回数が所定値を超過したと判定された場合に、中継装置１０は、隣接中継装置から受信したシグネチャを当該隣接中継装置を除く他の隣接中継装置に対して送信する。
【選択図】　図１

出願人履歴

０００００４２２６
19990715
住所変更
５９１０２９２８６

東京都千代田区大手町二丁目３番１号
日本電信電話株式会社